

REMARKS

Please reconsider the present application in view of the following remarks. Applicant thanks the Examiner for carefully considering the present application.

Disposition of Claims

Claims 1-35 are pending in this application. Claims 1, 17, 18, 34, and 35 are independent. The remaining claims depend, directly or indirectly, from claims 1, 17, 18, 34, and 35. Claim 21 has been cancelled by this reply.

Drawings

Applicant respectfully requests the Examiner to acknowledge whether the formal drawings filed on December 21, 2001 are acceptable.

Rejection(s) under 35 U.S.C § 101

Claims 18-35 were rejected under 35 U.S.C. § 101 because the claimed invention as disclosed is inoperative and therefore lacks utility. For the reasons set forth below, the rejection is respectfully traversed.

The Examiner asserts that independent claims 18, 34, and 35, teach the encryption key is hashed and stored presumably for future manipulation. The Examiner further asserts Applicant's method and apparatus does not have any use because the encryption key cannot be recovered. (See Office Action dated November 24, 2004 at page 3). Applicant acknowledges hash functions are one-way functions and one-way functions are "secure" in that an inverse operation does not exist. However, Applicant respectfully asserts that the encryption key is hashed and stored for future access (as needed), *not* manipulation. The hashed encryption key remains hashed and is only accessed in hashed form. Accordingly, an inverse operation is not required and, contrary to the Examiner's assertion, Applicant's method and apparatus does have use. Furthermore, amended claims 18 and 34 make use of both data and an algorithm to produce a concrete, tangible, and useful result (*e.g.*, an encrypted serial

file accessible only to those with the key encryption key). Thus, Applicant respectfully asserts that claims 18-35 are directed to statutory subject matter and has utility. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 112

Claims 18-35 stand rejected under 35 U.S.C. § 112, paragraph two, as being indefinite for failing to distinctly point out and claim the subject matter of the invention. Reconsideration of the rejection is respectfully requested.

The Examiner has asserted that independent claims 18, 34, and 35, teach the encryption key is hashed and stored presumably for future manipulation. (*See* Office Action dated November 24, 2004 at page 4). Applicant acknowledges hash functions are one-way functions and one-way functions are “secure” in that an inverse operation does not exist. Applicant respectfully asserts it would be clear to one with ordinary skill in the art that the encryption key of the present invention is hashed and stored for future access, *not* manipulation. Thus, no inverse operation of the hash is contemplated by the invention. Specifically, once hashed, the encryption key is sufficiently secure to be stored, and is only accessible in its hashed form (*See, e.g.,* Instant Specification at [0026]). Thus, it is clear that claims 18, 34, and 35 are sufficiently definite and patentable. Claims 19-33 depend, either directly or indirectly, from claim 18 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 24 and 25 also stand rejected under 35 U.S.C. § 112, because the Examiner asserts that Applicant improperly refers to a “tuple” with more than two elements. (*See* Office Action dated November 24, 2004 at page 4). Applicant respectfully asserts it would be clear to one of ordinary skill in the art that a “tuple” refers to a data object of two or more components. As evidence, Applicant has attached a definition of “tuple” from an online dictionary (www.hyperdictionary.com) to this response. Further, the term “tuple” as used by Applicant in the Instant Specification (at [0031]) and as shown in Figure 4 is a tuple with 3 data fields. Thus, the term used in claims 24 and 25, properly read in light of the specification, should

not be limited to a pair. Thus, it is clear that claims 24 and 25 are sufficiently definite and patentable. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 21, 34, and 35 stand rejected under 35 U.S.C. § 112, because the claims recite the limitation “the secret tokens” for which there is insufficient antecedent basis. Claim 21 has been cancelled and therefore the rejection is moot as to that claim. Claims 34 and 35 have been amended to clarify the invention recited. Accordingly, withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C § 102

Claims 1-9, and 17 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,673,316 issued to Auerbach et al. (hereinafter “Auerbach”). This rejection is respectfully traversed.

For anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Applicant respectfully asserts that Auerbach does not teach or suggest all the limitations recited in the amended independent claims 1 and 17.

Independent claims 1 and 17 have been amended to add the limitation “wherein data is used to generate a key in the key management system.” Specifically, the interface taught by Auerbach provides a means for inputting data into the key management system to access data already encrypted by part encryption keys (PEKs). Thus, the interface in Auerbach is only used when the encryption keys *have already* been generated and the data *has already* been encrypted. In contrast, the interface recited in the claims provide a means for inputting data into the key management system, wherein the data is then used *to generate* the encryption keys because the encryption keys *have not yet been* created (*See* Instant Specification at [0034]). Thus, it is clear that amended claims 1 and 17 are now patentable over Auerbach. Claims 2-9 depend, either directly or indirectly, from claim 1 and are allowable for at least the same reason. Accordingly, withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C § 103

Claims 10-16 and 18 stand rejected under 35 U.S.C. § 103(a) as rendered obvious by U.S. Patent No. 5,673,316 issued to Auerbach et al. (hereinafter "Auerbach"). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Applicant's disclosure. See MPEP section 706.02(j).

Because claim 1 is allowable for the reasons argued by Applicant above for the rejection under 35 U.S.C. § 102(b), claim 10 (which depends directly from claim 1), is also allowable. Auerbach, whether considered separately or in combination fails to teach or suggest claim 10. Claims 11-16 depend, either directly or indirectly from claim 10, and are patentable for at least the same reason. Accordingly, withdrawal of this rejection is respectfully requested.

The Examiner has rejected claim 18 asserting that it would be obvious to one of ordinary skill to apply compression algorithms to the cryptographic envelope allegedly taught in Auerbach, to reduce storage and thereby facilitate more efficient transmission over networks such as the internet. (See Office Action dated November 24, 2004 at page 7). The Examiner has attempted to equate this compression algorithm to the step of serializing a vector as recited in claim 18. Applicant respectfully acknowledges that serialization is the flattening of an n-dimensional object in to a one-dimensional object or "vector" and that the cryptographic envelope as taught by Auerbach is an n-dimensional object. However, serialization, as recited in claim 18, does *not* reduce storage or facilitate transmission;


instead, serialization causes the data to be stored as a serial file in order to persist beyond the time the Key Management System KMS is active. (See Instant Specification at [0030]). Clearly, the compression algorithm in Auerbach does not teach or suggest serializing as recited in claim 18. Furthermore, although claim 10 should already be deemed allowable for the reasons stated above, Auerbach also does not teach or suggest serializing as recited in claim 10. Claims 11-16 depend, either directly or indirectly from claim 10, and are patentable for at least the same reason. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/010001).

Dated: February 24, 2005

Respectfully submitted,

By 

Robert P. Lord
Registration No.: 46,479
OSHA & MAY L.L.P.
1221 McKinney, Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant